UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF NEW YORK

OUSSAMA EL OMARI, Plaintiff, -against- DECHERT LLP, et al., Defendants.	:	23-CV-4607 (LAK) (OTW) **REPORT AND RECOMMENDATION TO THE HONORABLE LEWIS A. KAPLAN**

ONA T. WANG, United States Magistrate Judge:

This case has been referred to me for general pretrial management and reports and recommendations for dispositive motions. (ECF 14). All three Defendants, Dechert LLP ("Dechert"), and Nicholas Paul Del Rosso ("Del Rosso") and Vital Management Services, Inc. ("Vital") (Del Rosso and Vital, collectively, the "Vital Defendants"), have filed motions to dismiss. (*See* ECF Nos. 34 and 36).[1] For the reasons set forth below, I respectfully recommend that Defendants' motions be **GRANTED** and the case be **DISMISSED** in its entirety.

I. BACKGROUND

Plaintiff has previously filed two other actions in this District concerning his disputes with governmental agencies from Ras Al Khaimah ("RAK"), one of seven emirates composing the United Arab Emirates ("UAE"). *See El Omari v. Kreab (USA), et al.*, No. 16-CV-3895 (NRB) and *El Omari v. Buchanan, et al.*, No. 20-CV-2601 (VM). This background is drawn from the dockets and filings in the prior cases and the instant Complaint. (ECF 1) (hereinafter "Compl.").

[1] Briefing on Dechert's motion to dismiss (ECF 36) is located at ECF 37, 38, 50, 51, and 71. Briefing on the Vital Defendants' (Del Rosso and Vital) motion to dismiss (ECF 34) is located at ECF 35, 40, 52, 53, 56, 57, 64, 72, and 73.

A. El Omari I: *El Omari v. Kreab (USA), et al.*, No. 16-CV-3895 (NRB)[2]

In 2016, Plaintiff, Oussama El Omari ("Plaintiff" or "El Omari"), through his counsel, Scott Moore, sued the RAK Free Trade Zone Authority ("RAKFTZA")[3] (and others) in connection with Plaintiff's termination of employment, and civil and criminal suits[4] brought against Plaintiff, *in absentia*, in the RAK. (El Omari I, ECF 1). In *El Omari I*, Plaintiff brought a fraud claim against The Arkin Group ("TAG") for preparing an unfavorable report in 2011 that apparently contributed to Plaintiff's 2012 termination from his position as Director of the RAKFTZA. (El Omari I, ECF 30, Second Amended Complaint) ("SAC"). As relevant here, in his Proposed Third Amended Complaint, Plaintiff also sought to bring hacking claims against RAKFTZA and Sheikh Saud under the Computer Fraud and Abuse Act ("CFAA"), 18 U.S.C. § 1030 *et seq.*, for the March 15, 2014, hacking of Plaintiff's personal website. (El Omari I, ECF 121-1 at 32-34; *see also* ECF 135 at 33). Dechert was a law firm of record for RAKFTZA and for Sheikh Saud. (*See* docket report for El Omari I). On August 18, 2017, in a 43-page opinion, Judge Buchwald dismissed the SAC, denied Plaintiff leave to amend to add his CFAA claim, and denied Plaintiff's and TAG's cross motions for sanctions. (El Omari I, ECF 135). Judge Buchwald's dismissal was affirmed in all respects by the

---

[2] The Court adopts the abbreviations and acronyms consistent with their use in prior Court opinions in *El Omari v. Kreab, et al.* ("El Omari I"), No. 16-CV-3895 (NRB), and *El Omari v. Buchanan, et al.* ("El Omari II"), No. 20-CV-2601 (VM).

[3] RAKFTZA is an agency or instrumentality of RAK. (*See* El Omari I, ECF 164 at n.1).

[4] Plaintiff alleged, *inter alia*, in *El Omari I* that his termination was politically motivated and part of a political power struggle between Sheikh Faisal bin Saqr Al Qassimi and his brother, Sheikh Saud, and that after Sheikh Saud obtained control of RAKFTZA, that Plaintiff was tried and convicted *in absentia* by the Criminal Court of RAK, and that his criminal conviction caused Interpol to issue a red notice on request of the UAE. *See El Omari v. Int'l Crim. Police Org.*, 35 F. 4th 83, 86 (2d Cir. 2022) (affirming dismissal for lack of subject matter jurisdiction), *cert. denied*, 143 S. Ct. 214 (2022). This red notice resulted in Plaintiff missing a connecting flight after he was temporarily detained after re-entering the United States. *Id*. After Interpol declined to remove or modify the red notice, Plaintiff also sued Interpol in the Eastern District of New York for "negligent infliction of emotional distress and violation of his right to due process of law under the New York State Constitution." *Id*. at 85.

Second Circuit on August 23, 2018, *El Omari v. Kreab (USA) Inc.*, 735 F. App'x 30, 32 (2d Cir. 2018), and the Supreme Court denied *certiorari* on February 19, 2019. *El Omari v. Ras Al Khaimah Free Trade Zone Auth.*, 139 S. Ct. 1170 (2019).

B. El Omari II: *El Omari v. Buchanan, et al.*, No. 20-CV-2601 (VM)

On March 27, 2020, Plaintiff, with the same counsel, sued several defendants, including Dechert and two of its London-based attorneys, again relating to his former employment with RAKFTZA. (El Omari II, ECF 1). Specifically, Plaintiff claimed that numerous defendants engaged in a civil RICO conspiracy to make multiple false and defamatory statements about him. (El Omari II, ECF 95 at 3-6). Plaintiff also brought a hacking claim under the CFAA alleging that a person named Samantha Alison ("Alison") posed as a Fox News journalist and communicated with Plaintiff by email, telephone, and Skype several times beginning in February 2020. *Id*. at 6-7. As a result of those communications, Plaintiff alleged, he provided Alison with the "contact information for five individuals and a copy of a confidential letter from El Omari's counsel to DHS." *Id*. By late April 2020, Plaintiff discovered that Alison "was an imposter and [had] used a fake email address;" that Alison "accessed his computer," and claimed that Alison was Defendants' agent. *Id*. at 7. In dismissing the complaint, on December 10, 2021, Judge Marrero found that Plaintiff had failed "to plausibly allege that Defendants – as opposed to someone else – were responsible for any purported hacking" of Plaintiff's computer, or that they had "conspired with Alison for that purpose." *Id*. at 42. Judge Marrero further found that Plaintiff

had failed to plausibly allege "injury" or "access"[5] under the CFAA and *Van Buren v. United States*, 141 S. Ct. 1648, 1660 (2021).[6] The Second Circuit affirmed on September 26, 2022, *El Omari v. Buchanan*, No. 22-55-CV, 2022 WL 4454536, at *3 (2d Cir. 2022).

C. 2022 Motion to Reopen *El Omari I*

On August 29, 2022, Plaintiff filed a motion to reopen *El Omari I* under Fed. R. Civ. P. 60(b), arguing that a January 6, 2022, post-trial affidavit by Stuart Robert Page (the "Page Affidavit"), filed in a separate English litigation, constituted new, "undisclosed evidence," and a change in United States policies regarding "transnational repression" warranted reopening of the intentional infliction of emotional distress claim against Sheikh Saud. (El Omari I, ECF 164 at 9-12). Judge Buchwald denied the motion as untimely, stating that "plaintiff's repeated, unsuccessful bites at the proverbial apple – weigh heavily in favor of finality." *Id*. at 17.[7]

Despite denying the motion on procedural grounds, Judge Buchwald also addressed the substance of Plaintiff's arguments, pointing out that Plaintiff's submissions did not raise anything new, because he has repeatedly claimed that he had been targeted by Sheikh Saud through Interpol red notices and foreign legal proceedings. *Id*. at 19-20. Further, even if he were

[5] As to "access," Plaintiff had alleged that the email and Skype communications – without any pleading that these communications contained malware – constitute access. Judge Marrero found that this was not sufficient. (El Omari II, ECF 95 at 44-48, n.11).

[6] *See Omari II*, ECF 90, Notice of Supplemental Authority, attaching *Van Buren* as Exhibit A. When directed to respond, Plaintiff filed ECF 92 to address the interpretation of *Van Buren,* and attached his own "supplemental authority," a criminal information and deferred prosecution agreement — against an apparently unrelated individual in a different jurisdiction — to suggest that spearphishing "technologically now can be done 'zero click' (i.e., not requiring a user to click anything[.])" (ECF 93 at 1). The Court notes that the criminal information uses the phrase "zero-click computer hacking and intelligence gathering system" in a different portion of the information from the discussion of spearphishing, and specifically defines "spearphishing" to use emails and documents "containing malware embedded within a message or attachment." (ECF 93-1 ¶¶ 56, 62(a)).

[7] The Second Circuit also denied Plaintiff leave to amend his complaint based on the Page Affidavit. Instead, the court specifically determined that "[t]he Page Affidavit addresses potential misconduct only in foreign proceedings and investigations conducted by RAK." *El Omari*, 2022 WL 4454536, at *2.

in fact targeted by Sheikh Saud, that his hardships "stem from unrelated, foreign legal proceedings which may not be challenged directly in this Court." *Id*. at 22-23.[8]

D. El Omari III: *El Omari v. Dechert LLP, et al.*, No. 23-CV-4607 (LAK)

The Complaint in this action, "*El Omari III*," was filed on June 1, 2023, suing Dechert, Sheikh Saud's prior counsel in *El Omari I*, Vital Management, Dechert's investigative firm, and Nicholas Del Rosso, Vital's principal private investigator. (Compl. at 2-3). It contains three claims: (1) hacking under the CFAA, 18 U.S.C. § 1030(a)(2)(C); (2) conspiracy to commit hacking under the CFAA, 18 U.S.C. § 1030(b); and (3) conversion under North Carolina law, in connection with an apparent hack of one of Plaintiff's email accounts. *Id*. at 18-26. This hacking apparently arises from Plaintiff's receipt and response to a phishing email dated January 3, 2017, sent by "Matt Rosen," containing a purported invitation to speak at "Adobe Summit EMEA 2017." *Id*. at ¶¶ 23, 25. A few days later, after Plaintiff declined the invitation, "Matt Rosen" sent another email containing an attachment which, after Plaintiff clicked on it,[9] installed malware that stole Plaintiff's Outlook email credentials. *Id*. at ¶¶ 26-27.

Notwithstanding the phishing emails and two prior claims of CFAA hacking, Plaintiff claims that he was unaware of any hacking of his emails until January 13, 2023, when he was

[8] Judge Buchwald continued: "No doubt recognizing this, plaintiff attempted to turn the helpful advice provided by Customs agents at JFK into a cause of action in 2017 and now hopes to revive the claim. Indeed, it is difficult to believe that El Omari would have preferred to remain unaware of the red notice and convictions pending against him in the event that he considered a return visit to the UAE or travel to a country likely to honor the red notice." *Id*. at 23.

[9] Plaintiff asserts that after he clicked on the link, he "saw a page of computer language he did not understand" and that "[i]t is consistent with such a malicious website that when El Omari clicked on this first link, malware with the capability to steal his login credentials was automatically downloaded onto El Omari's computer." (Compl. ¶ 27).

notified[10] that confidential emails between Plaintiff and his counsel, Scott Moore, had been found on a laptop located in the United Kingdom[11] that belonged to Defendant Del Rosso (the "Del Rosso Laptop"). *Id*. at ¶¶ 19-20, 45. Two other devices were also described in the UK Notice, including a hard drive claimed by Dechert and a hard drive claimed by Buchanan, one of the defendants in *El Omari II*. *Id*. at ¶ 21.

Plaintiff asserts that the presence of a "tranche" of confidential emails between Plaintiff and his counsel found on the Del Rosso Laptop means that the Defendants engaged in hacking of Plaintiff's email accounts. *Id*. at ¶ 20.

II. PROCEDURAL POSTURE

Plaintiff instituted *El Omari III* on June 1, 2023, by filing the Complaint (ECF 1) and a motion for preliminary injunction (ECF 6). The next day, the case was referred to me for general pretrial purposes and reports and recommendations on dispositive motions. (ECF 14). A case management conference was scheduled for October 3, 2023, while the parties engaged in discussions concerning briefing the motions to dismiss and addressing the motion for preliminary injunction. (*See* ECF 55). During the summer, Plaintiff and Dechert entered into a stipulation that mooted the preliminary injunction as to any of Plaintiff's hacked emails that might be in Dechert's possession, custody or control. (*See* ECF 29).[12] Plaintiff was unable to

[10] Compl. ¶ 19 ("On January 13, 2023 . . . El Omari's undersigned counsel received a foreign notice pursuant to a U.K. court order, concerning disclosure in London of the discovery of the three data storage devices. ("the [UK] [N]otice").").

[11] There are several actions pending in the UK, S.D.N.Y., and M.D. N.C. that relate to acts taken by RAK entities against Plaintiff and others, which the Court discussed at the conference on October 3, 2023. (ECF 65, Transcript of October 3, 2023 Conference).

[12] Without admitting whether Dechert was in possession of any allegedly hacked emails, they agreed on August 21, 2023, to preserve the same. (ECF 29 at 1).

reach a similar agreement with Vital and Del Rosso, however, which then led to a (somewhat incomprehensible) "emergency motion for temporary restraining order" in letter form on September 7, 2023. (ECF 42). In the emergency motion, Plaintiff apparently takes issue with the process proposed in the UK[13] to extract and delete Plaintiff's emails from the Del Rosso Laptop. *Id*. at 2 ("Moreover, the Vital Defendants extraction plan would destroy the only evidence (a forensic image) showing how the subject emails came to be on the Laptop.").

Dechert's motion to dismiss, filed on August 25, 2023, is straightforward: Plaintiff has again failed to plead any claims under the CFAA, and the conversion claim is time-barred. (ECF 37 at 12-22). In their motion to dismiss, also filed on August 25, 2023, the Vital Defendants add a jurisdictional defense as well as arguments for denying the preliminary injunction. (ECF 35 at 19-24, 31-38). Plaintiff has also sought leave to file additional exhibits to "supplement" and add "new evidence in support of the allegations in the complaint and Plaintiff's motions for preliminary injunction and TRO." (ECF 74 at 2). The proffered "evidence" is not to be considered on a motion to dismiss, and I will address the motions for preliminary injunction and TRO separately.

For the reasons below, I respectfully recommend that the Defendants' motions to dismiss be **GRANTED**, and I will address Plaintiff's motions for preliminary injunction and temporary restraining order in a separate Report and Recommendation, if necessary.

[13] There are apparently seven (or more) proceedings in the UK that may be related to acts taken by RAK in the same time frame as the acts in *El Omari I*. (ECF Nos. 61-1 and 65). As relevant here, Plaintiff's claim for hacking arises from the UK Notice that disclosed that confidential emails dated around 2017 were found on the Del Rosso Laptop, and Plaintiff's objection to the proposed, UK court-supervised method of disposing of the confidential materials before returning the devices to their owners.

III. ANALYSIS

A. Personal Jurisdiction (Vital Defendants)

The Vital Defendants argue that Plaintiff has not pleaded sufficient facts to establish personal jurisdiction. This Court has personal jurisdiction over any defendant "who is subject to the jurisdiction of a court of general jurisdiction in the state where the district court is located," here New York. *See* Fed. R. Civ. P. 4 (k)(1)(A). Under New York law, a court has specific jurisdiction over a foreign party if that party "transacts any business within the state" or "commits a tortious act within the state," and those acts give rise to the claim. *See* N.Y. C.P.L.R. § 302(a). This is a two-part inquiry: first, does the New York long-arm statute confer jurisdiction, and if so, does exercise of that jurisdiction comport with due process?

The Complaint alleges that Defendant Del Rosso was hired by David Neil Gerrard,[14] an attorney in Dechert's London office, in relation to Dechert's representation of Sheikh Saud and various "RAK governmental entities under his authority." (Compl. ¶ 5). Thus, because Del Rosso acted as a private investigator for Dechert, Del Rosso was an agent for Dechert. Finally, because Dechert was defense counsel in *El Omari I*, and a defendant in *El Omari II*, and because "on information and belief," Del Rosso must have personally attended meetings in New York, he must have been transacting business under New York's long arm statute, "easily sufficient to exercise general and specific jurisdiction." (Compl. ¶ 13-15; ECF 56 at 15). There is no pleading of facts to support jurisdiction over Vital other than general allegations of Del Rosso's control over Vital. (Compl. ¶ 5-6).

[14] Dechert and Gerrard were defendants in *El Omari II*.

The allegations in the Complaint do not satisfy either the "transacting business" or "tortious act" part of the statute. At best, Del Rosso – like Plaintiff, a domiciliary of North Carolina – was hired by a London-based Dechert attorney as an investigator for parties adverse to Plaintiff's interests in RAK, for which Plaintiff brought suit in this District. The RAK-based defendants were represented by New York-based Dechert attorneys. Del Rosso traveled to New York to deliver a "secure drive" and may have traveled to New York at other times for other unspecified reasons.[15] There is no pleading that either a business transaction giving rise to the injury or a tort was committed by Del Rosso in New York. These facts, even if all true and properly presented for consideration, are not sufficient to allege specific jurisdiction, let alone general jurisdiction.

The allegation of Del Rosso's participation in the "massive investigation," at Dechert's direction since 2014, fares no better: even if true, Del Rosso's work in the investigation did not lead to acts in New York. Nowhere does the Complaint allege that Plaintiff's termination or the trials *in absentia* in RAK occurred in New York, let alone that Del Rosso played any role in those acts. At best, Plaintiff alleges, with zero factual support, that the hacked emails were "used by" Dechert's New York lawyers in *El Omari I*. (Compl. ¶ 39). But this also cannot be possible, because *El Omari I* was dismissed at the pleading stage. Plaintiff himself is a non-domiciliary,

[15] Perhaps understanding that such conclusory pleading is not sufficient, Plaintiff argues in his opposition brief that "there are two specific facts adding to the complaint allegations that point to Del Rosso's business activity in the State of New York." (ECF 56 at 12). Plaintiff asserts that Del Rosso testified in the UK Litigation that he traveled to New York to deliver a "secure drive" and that he admitted to participating in a "massive investigation" of Plaintiff as directed by Dechert. *Id*. at 13-15. He cites no law to suggest that supplemental allegations of facts in an opposition brief can be considered by the Court on a motion to dismiss. Again, it is pure speculation that the "secure drive" delivered to New York "gave rise" to the events complained of here, and the hacking is not alleged in the Complaint to have occurred here, nor is it alleged to have been done by Del Rosso in New York (or anywhere). *Id*.

and he does not allege any injury in this District, except (perhaps) losing a litigation that he chose to bring here.

Accordingly, Del Rosso and Vital should be **DISMISSED** for lack of personal jurisdiction.[16]

B. Statute of Limitations

The private right of action under the CFAA is governed by a two-year statute of limitations. 18 USC § 1030(g). The conversion claim is governed by a three-year statute of limitations over which the discovery rule does not apply. *See, e.g.*, *White v. Consolidated Planning*, 166 N.C. App. 283, 310 (N.C. 2004) (discovery rule does not apply to conversion claims); *see also Azima v. Del Rosso*, No. 20-CV-954, 2021 WL 5861282, at *5 (M.D. N.C. Dec. 10, 2021). *Sewell v. Bernardin*, cited by none of the parties addressing a CFAA statute of limitations argument, is the only Second Circuit opinion to apply the CFAA's two-year statute of limitations. 795 F.3d 337 (2d Cir. 2015). In *Sewell*, the plaintiff's ex-boyfriend obtained her passwords while a guest in her home, accessed her AOL and Facebook accounts, and changed their passwords. *Id*. at 338-39. The plaintiff alleged that she only realized that her accounts had been hacked when she tried to access them and found that the passwords had been changed; shortly after discovering she no longer had access to those accounts, those accounts were used to post malicious statements about her. *Id*. The Second Circuit found that the two-year statute of limitations began to run from the date she discovered – for each account — that she could no longer access her accounts. Internet records "confirmed that [defendant's] computer was used

[16] The Vital Defendants also assert that Plaintiff cannot establish venue under 28 U.S.C. § 1391(b)(1) because neither Del Rosso nor Vital live in New York, and cannot establish venue under § 1391(b)(2) because "Plaintiff essentially concedes that venue is lacking in this jurisdiction by alleging that the hacking giving rise to Plaintiff's damages occurred outside both this District and indeed outside the United States." (ECF 35 at 24).

to gain access to the servers on which [plaintiff's] accounts were stored," after which he changed her passwords. *Id*. at 339.

Here, Plaintiff's investigation commenced after he received the UK Notice in 2023 that a "tranche" of emails from 2017 had been found on the Del Rosso Laptop.[17] (Compl. ¶ 20). Plaintiff's investigation apparently found that he had received phishing emails in 2017 inviting him to speak at a conference. *Id*. at ¶ 25. After Plaintiff initially declined, "Matt Rosen" sent Plaintiff an attachment containing links that purported to be links to videos of other, past speakers, ostensibly to convince Plaintiff to agree to the speaking engagement. *Id*. at ¶ 26. But, as Plaintiff alleges, these links were not videos, and clicking on them caused malware to be installed on Plaintiff's computer(s), which allowed the hacker to access Plaintiff's email account, ceo@oussamaelomari.com, and save or copy several privileged communications between Plaintiff and his counsel. *Id*. at ¶ 27. Specifically, **on or around January 12, 2017**, Plaintiff opened the document attached to the email and then clicked on a link embedded in the document "and saw a page of computer language he did not understand." *Id*. This result is "consistent with such a malicious website that when [Plaintiff] clicked on [the] link, malware with the capability to steal his login credentials was automatically downloaded onto [Plaintiff's] computer." *Id*.

Plaintiff asserts that the statute of limitations for both conversion and the hacking claims only began to run in 2023, when Plaintiff received the UK Notice. *Id*. at ¶¶ 50, 62. I disagree. The "damage," as pleaded in the Complaint, was the installation of the malware onto Plaintiff's

[17] The Del Rosso Laptop was not alleged to be an instrument of the hacking, because it was manufactured in 2019. (Compl. ¶ 20).

computer, not the access or "damage" to an Outlook server maintained elsewhere since, by his own pleading, the malware was automatically downloaded when Plaintiff clicked on the link on or around January 12, 2017. *See* 18 USC § 1030(e)(8) (defining "damage" as "any impairment to the integrity or availability of data, a program, a system, or information"); *Cf. Sewell*, 795 F.3d at 340 (passwords were not stolen by malware in 2011 incident; finding damage and unauthorized access occurred when defendant accessed plaintiff's accounts and changed her passwords).

Nor is it plausible to find that the "discovery of the damage" occurred when Plaintiff received the UK Notice in 2023, or after he conducted an investigation after receiving the UK Notice. *See Verschleiser v. Frydman*, No. 22-CV-7909 (JGK), 2023 WL 5835031, at *8 (S.D.N.Y. Sept. 7, 2023) (finding CFAA claims untimely because it was "implausible that the plaintiff could not have discovered the source of the injury" where results of hacking would have been apparent years previously, and plaintiff did not plead when he discovered the intrusion). Here, Plaintiff discovered the intrusion in January 2017, as soon as he clicked on the link – which was embedded in an attachment that was attached to an email sent from someone he did not know – when the link did not open, and his computer screen filled with "a page of computer language he did not understand." (Compl. ¶ 27). Plaintiff is no stranger to hacking claims or in the retention of "computer experts" to investigate hacking, even in the time period shortly after he clicked the link that caused the malware to be installed: in his proposed Third Amended Complaint in *El Omari I*, Plaintiff claimed that his "computer expert" had created a document dated January 25, 2017, that indicated that his personal website had been hacked in 2014. (El Omari I, ECF 121-1 at ¶¶ 84-93). Accordingly, the damage was discovered in 2017, more than six years before this action was commenced, and all of the claims should be **DISMISSED** as

untimely. To find otherwise would nullify the limitations period in 18 USC § 1030(g),[18] encourage a willful ignorance of phishing and other hacking techniques, and reward a lack of basic cyber security awareness.[19]

C. Dismissal for Failure to State a Claim

Even if the Vital Defendants were subject to personal jurisdiction here, and even if one could find that the malware installation was not "discovered" until Plaintiff was told that confidential emails had been disseminated to others, the Complaint fails to state a claim as to all Defendants, for largely the same reasons that Plaintiff's prior unsuccessful hacking claims were dismissed in *El Omari II*.

1. Standard of Review

For the purpose of deciding a motion to dismiss pursuant to Fed. R. Civ. P. 12(b)(6), the Court must accept all allegations in the complaint as true, and draw all reasonable inferences in

[18] The Court notes that claims under the Stored Communications Act and the Electronic Communications Privacy Act, which were considered in *Sewell* and *Verschleiser*, respectively, are also subject to a two-year statute of limitations, but based on the date upon which a plaintiff first has a "reasonable opportunity to discover" the intrusion or violation. Section 1030(g) does not impose a reasonableness requirement to the discovery of the hacking, nor have I read one into the statute. Rather, the discovery occurred when Plaintiff clicked on a link that did not take him to a video but filled his screen with "a page of computer language he did not understand." (Compl. ¶ 27).

[19] Plaintiff also argues that if the discovery rule does not apply, that Defendants should be equitably estopped from asserting a statute of limitations defense, since they were the ones who engaged in the hacking scheme. (*See* ECF 56 at 20-22). In order to rely on equitable estoppel, a plaintiff must plead facts to satisfy the following elements: "(1) conduct [by Defendants] . . . which amounts to a false representation or concealment of material facts; (2) the intention that such conduct will be acted on by the other party; and (3) knowledge, actual or constructive, of the real facts. The party asserting the defense must have (1) a lack of knowledge and the means of knowledge as to the real facts in question; and (2) relied upon the conduct of the party sought to be estopped to his prejudice." *Stratton v. Royal Bank of Canada*, 211 N.C. App. 78, 88 (N.C. App. 2011). Other than conclusory assertions in his opposition papers, Plaintiff has not pleaded conduct, intent, or knowledge of the real facts. Moreover, Plaintiff's act of clicking on the link from the unknown sender and the screen filling up with "computer language that he did not understand" is Plaintiff's knowledge and means of knowledge as to the real facts in question. New York law yields the same result: under New York law, equitable estoppel may apply to a conversion claim, but a plaintiff must allege "affirmative acts of concealment" that prevented him from bringing a suit earlier. *Su v. Sotheby's, Inc.*, No. 17-CV-4577 (VEC), 2022 WL 14118016, at *10 (S.D.N.Y. Oct. 24, 2022).

the plaintiff's favor. *McCarthy v. Dun & Bradstreet Corp.*, 482 F.3d 184, 191 (2d Cir. 2007). The Court's function on a motion to dismiss is "not to weigh the evidence that might be presented at a trial but merely to determine whether the complaint itself is legally sufficient." *Goldman v. Belden*, 754 F.2d 1059, 1067 (2d Cir. 1985). If the plaintiff has stated "enough facts to state a claim to relief that is plausible on its face," the complaint should not be dismissed. *Bell Atl. Corp. v. Twombly*, 550 U.S. 544, 570 (2007). "A claim has facial plausibility when the plaintiff pleads factual content that allows the court to draw the reasonable inference that the defendant[s] [are] liable for the misconduct alleged." *Ashcroft v. Iqbal*, 556 U.S. 662, 678 (2009). For a claim to sufficiently "raise a right to relief above the speculative level," it must be grounded on factual allegations. *Twombly*, 550 U.S. at 555. A claim grounded on mere suspicion is not enough to meet this standard. *Id*. "'[L]abels and conclusions' or 'a formulaic recitation of the elements of a cause of action will not do.' Nor does a complaint suffice if it tenders 'naked assertion[s]' devoid of 'further factual enhancement.'" *Iqbal*, 556 U.S. at 678 (quoting *Twombly,* 550 U.S. at 555, 557) (internal citation omitted, alteration in original).

Generally, "[w]hen considering a motion to dismiss, the Court's review is confined to the pleadings themselves," because "[t]o go beyond the allegations in the [c]omplaint would convert the Rule 12(b)(6) motion to dismiss into one for summary judgment pursuant to [Rule] 56." *Thomas v. Westchester Cnty. Health Care Corp.*, 232 F. Supp. 2d 273, 275 (S.D.N.Y. 2002) (citation omitted). However, "the Court's consideration of documents attached to, or incorporated by reference in the [c]omplaint, and matters of which judicial notice may be taken, would not convert the motion to dismiss into one for summary judgment." *Id.* (citations

omitted); *Maroney v. Woodstream Corp.*, No. 19-CV-8294 (KMK), 2023 WL 6318226, at *1 (S.D.N.Y. Sept. 28, 2023).

2. Counts One and Two: Hacking and Conspiracy to Commit Hacking (18 U.S.C. § 1030(a)(2)(C))

The CFAA, 18 U.S.C. § 1030 *et seq.*, in pertinent part, punishes an individual who "intentionally accesses a computer without authorization or exceeds authorized access, and thereby obtains . . . information from any protected computer." 18 U.S.C. § 1030(a)(2)(C). The CFAA was initially enacted solely as a criminal statute to address the "then-novel problem of [computer] hacking." *Hancock v. County of Rensselaer*, 882 F.3d 58, 63 (2d Cir. 2018). It was later amended to permit a civil cause of action allowing, among other things, "any person who suffers damage or loss by reason of a violation of this section" of at least $5,000 to bring a claim. 18 U.S.C. § 1030(g); § 1030(c)(4)(A)(i)(I); *accord Sewell*, 795 F.3d at 339–40; *Fischkoff v. Iovance Biotherapeutics, Inc.*, 339 F. Supp. 3d 408, 417–18 (S.D.N.Y. 2018) (cleaned up).

Plaintiff had previously sought to bring hacking claims in *El Omari I* (against RAKFTZA)[20] and *El Omari II* (against Dechert, a former London-based Dechert attorney, and others).[21] While he provides more detail this time, the allegations are still insufficient.

[20] In *El Omari I*, Counts VII (CFAA violation) and VIII (aiding and abetting CFAA violation) of Plaintiff's proposed Third Amended Complaint allege that El Omari's website was hacked in March 2014, "which deleted the entire website." (ECF 121-1 at ¶¶ 85(a), 90(a)). Plaintiff further alleged that hack "accessed and damaged" Plaintiff's computers that contained "the internal and confidential electronic data" of Plaintiff. *Id*. at ¶¶ 85, 90. Plaintiff named only RAKFTZA in these proposed counts, stating that RAKFTZA "directly and/or through its agents, knowingly and intentionally" caused or aided and abetted someone else in the alleged hack. *Id*.

[21] In *El Omari II*, Plaintiff alleges that he was misled by an "agent of" Dechert and the other defendants into giving five Skype interviews to someone he believed to be a Fox News journalist, that he provided this faux-journalist confidential information (including a "confidential attorney letter on behalf of" Plaintiff), and that her eliciting of this information via Skype constituted a violation under the CFAA. Judge Marrero additionally found that the acts by "Samantha Alison" did not constitute CFAA "access" under *Van Buren*.

First, Plaintiff does not allege that any Defendant accessed his computer, nor that any Defendant was affiliated with the hack. "A CFAA claim should be dismissed where plaintiffs provided no facts to establish that the defendant or any of its employees is affiliated with the hacks of plaintiffs' computers." (El Omari II, ECF 95 at 41) (quoting *Broidy v. Global Risk Advisors LLC*, No. 19-CV-11861, 2021 WL 1225949, at *9 (S.D.N.Y. Mar. 31, 2021)) (cleaned up). Plaintiff has previously brought two different CFAA claims, both of which were dismissed for, *inter alia*, failing to plead sufficient facts to establish that the defendants were responsible for the incidents. Here, Plaintiff again pleads "on information and belief" that Defendants were responsible for the phishing emails and the hacking. (Compl. ¶¶ 33, 35).

Plaintiff alleges sufficient facts that he was hacked by someone: he identifies the three phishing emails, the document containing the links, and that the link on which Plaintiff clicked pointed to a website that was created on the same day that the phishing email had been sent (January 12, 2017) and deleted on February 19, 2017. (Compl. ¶ 27). He further alleges that when he clicked on the link, the computer screen displayed "a page of computer language he did not understand," "consistent with" malware being downloaded on his computer. *Id*. In 2023, the Del Rosso Laptop was found to contain "a backup copy of emails containing the email address of"[22] Plaintiff's counsel. *Id*. at ¶ 19. Two other devices described in the UK litigations are claimed by Dechert and Del Rosso together, and by James Buchanan, another defendant in *El Omari II*. *Id*. at ¶ 21. These devices are not alleged to contain any email or email addresses of Plaintiff or his counsel. *Id*.

[22] Later, the description of the alleged hacked material is also called a "file," with a filename of "update24Jan.rar." (Compl. ¶ 20).

Although there is more detail about the hack itself, Plaintiff still does not plead facts to establish that Defendants – as opposed to someone else[23] – hacked or conspired to hack his emails. While Plaintiff pleads that Defendant Vital sent over $500,000 in wire transfers to an organization in India called CyberRoot in 2015 and 2016 (Compl. ¶ 33), the rest of the allegations attempting to link Defendants to the hacking are conclusory and made "upon information and belief." *See Leonard v. United States*, No. 23-CV-8571 (LTS), 2023 WL 8258263, at *3 (S.D.N.Y. Nov. 27, 2023) (beliefs, even strongly held, are not facts; complaint must set forth facts showing basis for information and belief). Plaintiff concludes, essentially, that Vital's payments to CyberRoot in 2015 and 2016 were for hacking of Plaintiff's emails, that Del Rosso provided names or email accounts (including Plaintiff's) to "Jain, the Indian hacking ringleader," and that "Jain's database is believed to also show that Del Rosso gave Jain over 40 hacking target names." (Compl. ¶ 33). The timing of these payments, months before and shortly after El Omari sued Defendants' clients, led Plaintiff to conclude that the hack in January 2017, was conducted to assist Dechert in defending its clients in *El Omari I*.

These are not plausible inferences to draw. First, Plaintiff does not connect either nonparty "Jain" or "CyberRoot" to the 2017 hacking incident in this case; rather, Plaintiff points to a 2022 report by Meta titled "Threat Report on the Surveillance-for-Hire Industry" that indicated that CyberRoot may have engaged in hacking and phishing activities on Facebook and Instagram. (Compl. ¶ 7). Second, with the exception of Vital's payments to CyberRoot in the

[23] Indeed, even after this suit was instituted, Plaintiff has sought to supplement his filings by sharing heavily redacted emails from an unknown individual, "KB," who appears to be in possession of more of Plaintiff's emails. (ECF 57-6). "KB" and their activities are not referenced in the Complaint, nor does Plaintiff explain why they are relevant or should be considered in opposition to a motion that considers whether the Complaint is facially sufficient under Fed. R. Civ. P. 12(b)(6).

year before the hacking, there is no connection drawn between Defendants and any hacker or hacking activity, whether by CyberRoot, Jain, or anyone else. Finally, as discussed briefly before, the hack occurred on January 12, 2017, after Dechert's clients and the other defendants had already filed their motions to dismiss. These motions to dismiss were granted at the pleading stage, and in particular, the claims against Dechert's clients, Sheikh Saud and RAKFTZA, were dismissed on immunity grounds. It is hard to see how emails between Plaintiff and his counsel, even if they had been obtained by Dechert during that time, could have affected their reply brief on sovereign immunity or the later appeals in *El Omari I*.

Plaintiff has also failed to plead financial loss greater than $5,000 under the statute. "Under the CFAA, a plaintiff must allege that he or she suffered one of five types of statutorily prescribed injuries." (El Omari II, ECF 95 at 42). As Judge Marrero explained, when reading *Van Buren* with previous cases, "the Supreme Court recently found that the statutory definitions of damage and loss focus on technological harms – such as the corruption of files – of the type unauthorized users cause to computer systems and data." *Id*. at 43 (cleaned up). The Complaint is still insufficient, pleading in vague and conclusory terms and includes not only "forensic computer investigation"[24] related to investigating and assessing the scope of the hacking, but legal fees and costs "seeking to remedy the complete loss of the confidentiality of the emails." (Compl. ¶ 41). The Complaint goes on to describe, in general and conclusory language, that Plaintiff suffered the "complete loss of valuable confidentiality . . . in the attorney-client

[24] It is also not clear whether all of Plaintiff's "forensic computer investigation costs" would be covered, since Plaintiff claimed in 2017, in *El Omari I*, that his personal website had been hacked in 2014, and claimed in *El Omari II* that he'd given five Skype interviews (and disclosed confidential information) in 2020 to someone who had posed as a reporter for Fox News.

communication emails pertaining to El Omari's NY litigation" (*id*. at ¶ 43), and, incoherently, "spending attorney fees and costs seeking to stop the use, dissemination of, and to restore the confidentiality of the emails on the [Del Rosso] Laptop from the Defendants." *Id*. at 42.

Notwithstanding Judge Marrero's instruction that damage under the CFAA should focus on the technological harms, (El Omari II, ECF 95 at 43), Plaintiff compares his hack to a data breach of IBM (ECF 56 at 29-30), to support his contention that he should be compensated for the loss of confidentiality of the emails with his attorney, going so far as to claim that attorney's fees attendant to his motion for preliminary injunction in this case are a covered loss. *Id*. at 28 ("The cost of obtaining injunctive relief in this case intended to restore the condition of confidentiality of his stolen emails incurred as a cost of responding to an offense and restoring the information to its condition prior to the offense."). The technological harm here was the apparent malware installation on Plaintiff's computer systems, and the Complaint does not sufficiently allege that the costs Plaintiff suffered were "from efforts to identify, diagnose, or address [that] damage." (El Omari II, ECF 95 at 44). Instead, he has continued to include the "value" of the confidentiality of Plaintiff's 2017 emails and efforts (including litigation) to "restore the confidentiality"[25] of the emails in his pleading of loss. These are not compensable

[25] It is further unclear what Plaintiff means when he seeks to "restore" confidentiality of the emails that were copied. The emails were disseminated to many, and that bell cannot be unrung. Restoring the security of his email accounts might have included changing passwords and other security measures after he clicked on the link, but it would be unreasonable to read the statute to mean that. In the 7 years since that incident, Plaintiff and his counsel (as well as counsel for defendants) have received emails from an anonymous "KB" who claims that all of Plaintiff's and his counsel's email accounts have been compromised. (*See* ECF 57-6). If that is true, then the destruction of emails on the Del Rosso Laptop would have no effect on "restoring confidentiality" of any communications that had been copied and disseminated since 2017.

under the plain language of the statute and *Van Buren*.[26]

3. Count Three: Conversion

Count Three – conversion under North Carolina law – is both time barred and fails to state a claim. As discussed above, the discovery rule does not apply to conversion claims under North Carolina law, and the "hack" occurred in January 2017. *Honeycutt v. Weaver*, 257 N.C. App. 599, 609 (N.C. 2018); *White*, 166 N.C. App. at 310 (N.C. 2004). But even if it were not time-barred, Plaintiff has not sufficiently pleaded that a conversion occurred. The North Carolina Supreme Court has defined the tort of conversion as "an unauthorized assumption and exercise of the right of ownership over goods or personal chattels belonging to another, to the alteration of their condition or the exclusion of an owner's rights." *Variety Wholesalers, Inc. v. Salem Logistics Traffic Services, LLC*, 365 N.C. 520, 523 (N.C. 2012) (internal citation omitted). Emails are neither goods nor personal chattels,[27] and Plaintiff's use of his email account apparently continued unimpeded.

Accordingly, Plaintiff's conversion claim should also be **DISMISSED**.

---

[26] Plaintiff quotes from *Van Buren*'s dicta about technological loss, and omits the last sentence, which makes clear that the "loss of privilege of" Plaintiff's emails is not recoverable damage. *Van Buren* examined whether a police officer could be held criminally liable for using information from a law enforcement database for a personal (and hence improper) purpose. In holding that he could not, the Supreme Court noted that the statute's definitions of "damage" and "loss" focused on technological harms from the hacking itself (the quoted language in Plaintiff's brief), to then say, "[t]he term's definitions are ill fitted, however, to remediating 'misuse' of sensitive information that employees may permissibly access from their computers. Van Buren's situation is illustrative: His run of the license plate did not impair the 'integrity or availability' of data, nor did it otherwise harm the database system itself." 141 S. Ct. at 1660 (internal citations omitted).

[27] Indeed, in *Van Buren*, the Supreme Court noted in dicta that "it became clear that traditional theft and trespass statutes were ill suited to address cybercrimes that did not deprive computer users of property in the traditional sense." 141 S. Ct. at 1652 (citing Kerr, *Cybercrime's Scope: Interpreting "Access" and "Authorization" in Computer Misuse Statutes*, 78 N.Y.U. L. Rev. 1596, 1605–1613 (2003)).

IV. CONCLUSION

For the reasons set forth above, I respectfully recommend that Defendants' motions be **GRANTED** and the case be **DISMISSED** in its entirety.

V. OBJECTIONS

In accordance with 28 U.S.C. §636(b)(1) and Fed. R. Civ. P. 72(b), the parties shall have fourteen (14) days (including weekends and holidays) from receipt of this Report to file written objections. *See also* FED. R. CIV. P. 6 (allowing three (3) additional days for service by mail). A party may respond to any objections within fourteen (14) days after being served. Such objections, and any responses to objections, shall be addressed to the Honorable Lewis A. Kaplan, United States District Judge. Any requests for an extension of time for filing objections must be directed to Judge Kaplan.

FAILURE TO FILE OBJECTIONS WITHIN FOURTEEN (14) DAYS WILL RESULT IN A WAIVER OF OBJECTIONS AND WILL PRECLUDE APPELLATE REVIEW. *See Thomas v. Arn*, 474 U.S. 140, 155 (1985); *IUE AFL-CIO Pension Fund v. Herrmann*, 9 F.3d 1049, 1054 (2d Cir. 1993); *Frank v. Johnson*, 968 F.2d 298, 300 (2d Cir. 1992); *Wesolek v. Canadair Ltd.*, 838 F.2d 55, 58 (2d Cir. 1988); *McCarthy v. Manson*, 714 F.2d 234, 237–38 (2d Cir. 1983).

Respectfully submitted,

/s/ Ona T. Wang
Ona T. Wang
United States Magistrate Judge

Dated: February 22, 2024
New York, New York